

# EVERY LENS SPACE CONTAINS A GENUS ONE HOMOLOGICALLY FIBERED KNOT

YUTA NOZAKI

**ABSTRACT.** We prove that every lens space contains a genus one homologically fibered knot, which is contrast to the fact that some lens spaces contain no genus one fibered knot. In the proof, the Chebotarev density theorem and binary quadratic forms in number theory play a key role. We also discuss the Alexander polynomial of homologically fibered knots.

## CONTENTS

1. Introduction	1
2. Homology cobordisms and proof of Theorem 1.1	2
3. Proof of Theorem 1.2	6
4. Homologically fibered knots and the Alexander polynomial	7
References	11

## 1. INTRODUCTION

It is well known that every connected oriented closed 3-manifold  $X$  contains a fibered knot. In other words,  $X$  admits an open book decomposition with connected binding. The minimum genus  $\text{op}(X)$  of pages of all open book decompositions of  $X$  is a fundamental invariant of  $X$ . For instance,  $\text{op}(X) = 0$  if and only if  $X \cong S^3$ . Morimoto [6] started to study genus one fibered knots (GOF-knots) in lens spaces, and Baker [2, Theorem 4.3] completely determined which lens space contains a GOF-knot, that is, we already know when  $\text{op}(L(p, q)) = 1$  holds. However, computation of  $\text{op}(X)$  is difficult in general.

Sakasai [8, Remark 6.10] introduced a homological analogue  $\text{hc}(X)$  of  $\text{op}(X)$ , which is roughly defined to be the minimum genus of surfaces  $\Sigma$  whose complements are homologically  $\Sigma \times [-1, 1]$ . Precisely,  $\text{hc}(X)$  is defined in terms of homology cobordisms or homologically fibered knots (see Definitions 2.2), and  $\text{hc}(X) \leq \text{op}(X)$  holds by definition. The author was informed by Sakasai the following sufficient condition for  $\text{hc}(L(p, q)) = 1$

---

2010 *Mathematics Subject Classification.* Primary 57M27, Secondary 11R45.

*Key words and phrases.* Homology cobordism; homologically fibered knot; density theorem; Alexander polynomial.

when  $q$  is odd:  $p(p+4)$  or  $p(p-4)$  is a quadratic residue mod  $q$ . The purpose of this paper is to prove the following theorem which enables us to compute  $\text{hc}(X)$  for various 3-manifolds  $X$  (see Corollary 2.5).

**Theorem 1.1.**  $\text{hc}(L(p, q)) = 1$  holds for any lens space  $L(p, q)$ , or equivalently  $L(p, q)$  contains a genus one homologically fibered knot.

It is shown in [8, Remark 6.10] that  $\text{hc}(X)$  depends only on the isomorphism class of the pair of  $H_1(X)$  and the torsion linking form  $\lambda_X: TH_1(X) \times TH_1(X) \rightarrow \mathbb{Q}/\mathbb{Z}$ , where  $TH_1(X)$  is the torsion subgroup of  $H_1(X) := H_1(X; \mathbb{Z})$ . The following example shows that  $\text{hc}(X)$  is not determined only by the isomorphism class of  $H_1(X)$ . For two 3-manifolds  $X_i = L(5, 1) \# L(5, i)$  ( $i = 1, 2$ ) whose torsion linking forms  $(1/5) \oplus (i/5)$  are not isomorphic, we have  $\text{hc}(X_1) = 1 \neq \text{hc}(X_2) = 2$  ([8, Remark 6.10]).

In order to prove Theorem 1.1, we should find a surface  $\Sigma \subset L(p, q)$  of genus one whose complement  $L(p, q) \setminus \text{Int}(\Sigma \times [-1, 1])$  is a homology cobordism. (It is easy to see that  $\text{hc}(X) = 0$  if and only if  $X$  is an integral homology 3-sphere.) The following theorem (to be proved in Section 3 by using the Chebotarev density theorem) and a well-known fact about binary quadratic forms allow us to construct a desired surface  $\Sigma$ .

**Theorem 1.2.** Let  $m \in \mathbb{Z}$  and  $n \in \mathbb{Z} \setminus \{0, 5\}$  be coprime. Then there exist  $\varepsilon \in \{1, -1\}$  and an odd prime  $l$  such that the congruent equation  $nx(x+1) \equiv \varepsilon \pmod{l}$  is solvable and  $l \equiv m \pmod{n}$ .

The study mentioned here is related to Goda and Sakasai's work [4] on homologically fibered knots. We discuss a homologically fibered knot (in a rational homology 3-sphere) and its Alexander polynomial in the last section. In this paper,  $L(p, q)$  denotes the lens space obtained from  $S^3$  by Dehn surgery on an unknot along the slope  $-p/q$ , where  $p \geq 2$  and  $q$  are coprime.

**Acknowledgments.** The author would like to thank Takuya Sakasai and Gwénaél Massuyeau for their various discussion. Also, he would like to express his gratitude to Mutsuro Somekawa and Ippei Nagamachi for their useful comments to prove Theorem 1.2. He wishes to be grateful to Institut de Recherche Mathématique Avancée, Université de Strasbourg, where most of this paper was written, for the hospitality. Finally, this work was supported by the Program for Leading Graduate Schools, MEXT, Japan and JSPS KAKENHI Grant Number 16J07859.

## 2. HOMOLOGY COBORDISMS AND PROOF OF THEOREM 1.1

We first review homology cobordisms following Garoufalidis and Levine [3, Section 2.4].

**Definition 2.1.** A *homology cobordism over  $\Sigma_{g,1}$*  is a triad  $(M, i_+, i_-)$ , where  $M$  is an oriented compact 3-manifold and  $i_+, i_-: \Sigma_{g,1} \rightarrow \partial M$  are embeddings satisfying

- $i_+$  is orientation-preserving and  $i_-$  is orientation-reversing;

- $i_+|_{\partial\Sigma_{g,1}} = i_-|_{\partial\Sigma_{g,1}}$ ;
- $i_+(\Sigma_{g,1}) \cup i_-(\Sigma_{g,1}) = \partial M$  and  $i_+(\Sigma_{g,1}) \cap i_-(\Sigma_{g,1}) = i_\pm(\partial\Sigma_{g,1})$ ;
- The induced maps  $(i_+)_*, (i_-)_*: H_*(\Sigma_{g,1}) \rightarrow H_*(M)$  are isomorphisms.

Note that the fourth condition is equivalent to the condition that  $M$  is connected and  $i_\pm$  induce isomorphisms on  $H_1(-)$ . Sakasai [8, Definition 6.9, Remark 6.10] introduced the following invariant of 3-manifolds by using homology cobordisms.

**Definition 2.2.** For a connected oriented closed 3-manifold  $X$ ,  $\text{hc}(X) \in \mathbb{Z}_{\geq 0}$  is defined by

$$\text{hc}(X) := \min\{g \in \mathbb{Z}_{\geq 0} \mid X \cong C_M \text{ for some } (M, i_+, i_-)\},$$

where  $C_M$  is the *closure* of a homology cobordism  $(M, i_+, i_-)$  over  $\Sigma_{g,1}$  defined by

$$C_M := M / (i_+(x) \sim i_-(x), x \in \Sigma_{g,1}).$$

For an embedding  $\iota: \Sigma_{g,1} \xrightarrow{\cong} \Sigma \subset X$ , we obtain the triad  $(X \setminus \text{Int}(\Sigma \times [-1, 1]), \iota^-, \iota^+)$ , where  $\iota^\pm := \iota \times (\pm 1)$ . Whether this triad is a homology cobordism or not depends only on the image of  $\iota$ , and we simply say that  $X \setminus \text{Int}(\Sigma \times [-1, 1])$  is a homology cobordism if the triad is so.

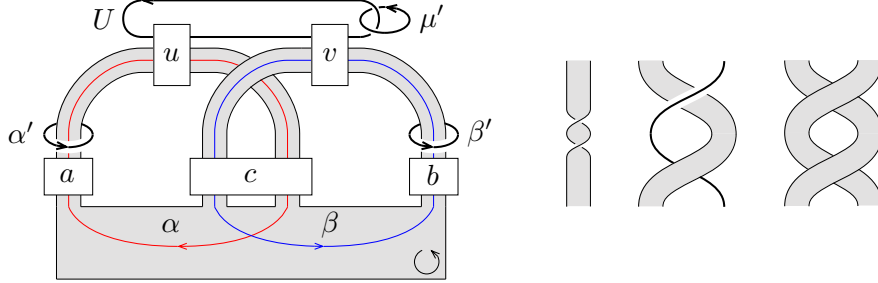


FIGURE 2.1. The surface  $\Sigma_{a,b,c,u,v}$  and unknot in  $S^3$ , where  $a, b, c, u, v \in \mathbb{Z}$ . The box with  $n \geq 0$  (resp.  $n < 0$ ) represents suitable  $n$  positive (resp. negative) full twists on the right.

The following key lemma is a corollary of Proposition 4.1, though we give a direct proof in this section. Note that for coprime integers  $p, q$  we can choose  $r, s \in \mathbb{Z}$  such that  $ps - qr = 1$ , then the others are written as  $r + kp =: r_k$ ,  $s + kq =: s_k$  for  $k \in \mathbb{Z}$ .

**Lemma 2.3.** *The complement  $L(p, q) \setminus \text{Int}(\Sigma \times [-1, 1])$  of the surface  $\Sigma = \Sigma_{a,b,c,u,v}$  illustrated in Figure 2.1 is a homology cobordism if and only if there exist  $\varepsilon \in \{1, -1\}$  and  $k \in \mathbb{Z}$  such that*

$$\begin{pmatrix} bu^2 + (2c+1)uv + av^2 \\ c^2 + c - ab \end{pmatrix} = \varepsilon \begin{pmatrix} r_k \\ s_k \end{pmatrix}.$$

*Proof.* It follows from the Mayer-Vietoris sequence for

$$L(p, q) \setminus \text{Int}(\Sigma \times [-1, 1]) = (S^3 \setminus \text{Int}(\Sigma \times [-1, 1] \cup N(U))) \cup_{\partial N(U)} N(U)$$

that  $H_1(L(p, q) \setminus \Sigma) \cong \text{Coker } \iota$ , where  $N(U)$  denotes a (closed) tubular neighborhood of the unknot  $U$  and  $\iota$  is the map

$$\iota: H_1(\partial N(U)) \rightarrow H_1(S^3 \setminus (\Sigma \cup N(U))) \oplus H_1(N(U)).$$

By the definition of Dehn surgery, the matrix of  $\iota$  with respect to the bases  $\{\mu, \lambda\}$ ,  $\{\alpha', \beta', \mu', \lambda\}$  is

$$A := \begin{pmatrix} qu & -su \\ -qv & sv \\ -p & r \\ 0 & 1 \end{pmatrix},$$

where  $\mu, \lambda$  denote a meridian and longitude on the torus  $\partial N(U)$  respectively.

Suppose that the complement is a homology cobordism, namely  $\{\alpha_\sigma, \beta_\sigma\}$  is a basis of  $\text{Coker } \iota$  for both  $\sigma = \pm$ , where  $\alpha_\pm := \alpha \times (\pm 1)$ ,  $\beta_\pm := \beta \times (\pm 1)$ . Then  $\{\alpha_\sigma, \beta_\sigma\}$  extends to a basis of  $H_1(S^3 \setminus (\Sigma \cup N(U))) \oplus H_1(N(U))$ . That is, there is a matrix  $Q_\sigma \in GL(4, \mathbb{Z})$  changing the basis  $\{\alpha', \beta', \mu', \lambda\}$  to a basis containing  $\alpha_\sigma, \beta_\sigma$ . We may assume that  $Q_\sigma$  is of the form  $Q'_\sigma \oplus (1)$ , where

$$Q'_+ = \begin{pmatrix} a & c & * \\ c+1 & b & * \\ u & -v & * \end{pmatrix}, \quad Q'_- = \begin{pmatrix} a & c+1 & * \\ c & b & * \\ u & -v & * \end{pmatrix}.$$

Since the  $(2 \times 2)$ -matrix at the bottom of the new matrix  $Q_\sigma^{-1}A$  of  $\iota$  must belong to  $GL(2, \mathbb{Z})$ , the absolute value of the  $(1, 3)$ -entry of  $Q_\sigma^{-1}A$  equals 1. Therefore, we may assume

$$(Q'_\pm)^{-1} \begin{pmatrix} qu \\ -qv \\ -p \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Then we have

$$Q'_+ = \begin{pmatrix} a & c & qu \\ c+1 & b & -qv \\ u & -v & -p \end{pmatrix}, \quad Q'_- = \begin{pmatrix} a & c+1 & qu \\ c & b & -qv \\ u & -v & -p \end{pmatrix}.$$

It follows from  $|\det Q'_\pm| = 1$  that

$$|p(c^2 + c - ab) - q(bu^2 + (2c+1)uv + av^2)| = 1.$$

This completes one direction, and the other is shown by reversing the above argument.  $\square$

Let us prove the main theorem by using Lemma 2.3, Theorem 1.2 (to be proved later) and the following fact (see, for example, [1, p. 37]): For  $n, \Delta \in \mathbb{Z}$ , the congruence equation  $z^2 \equiv \Delta \pmod{4n}$  is solvable if and only if there is a binary quadratic form  $f(x, y)$  with discriminant  $\Delta$  such that  $f(x, y) = n$  has a primitive solution.

*Proof of Theorem 1.1.* The case  $p = 5$  can be seen easily. Suppose  $p \neq 5$ . By setting  $m = r$ ,  $n = p$  in Theorem 1.2, we conclude that there are  $\varepsilon \in \{1, -1\}$  and  $k, a, b, c \in \mathbb{Z}$  such that  $px(x+1) \equiv \varepsilon \pmod{r_k}$  has a solution  $x = x_0$ . Here,  $z_0 := 1 + 2x_0$  satisfies  $z_0^2 \equiv 1 + 4\varepsilon s_k \pmod{4\varepsilon r_k}$ . By the above fact, there is a quadratic form  $f(x, y) = a'x^2 + b'xy + c'y^2$  such that  $b'^2 - 4a'c' = 1 + 4\varepsilon s_k$  and  $f(x, y) = \varepsilon r_k$  has a solution  $(x, y) = (u, v)$ . Then, integers  $a := c'$ ,  $b := a'$  and  $c := (b' - 1)/2$  satisfy

$$\begin{pmatrix} bu^2 + (2c+1)uv + av^2 \\ c^2 + c - ab \end{pmatrix} = \varepsilon \begin{pmatrix} r_k \\ s_k \end{pmatrix}.$$

Therefore, we conclude from Lemma 2.3 that  $\text{hc}(L(p, q)) = 1$ .  $\square$

**Remark 2.4.** It follows from the proof of the above fact about quadratic forms that integers  $a, b, c, u, v$  are represented by  $z_0, \varepsilon, r_k, s_k$ . However, it seems difficult to represent these integers explicitly by  $p, q$ .

We sum up values or estimates of  $\text{hc}(X)$  for some  $X$  as a corollary. Let  $d(G)$  be the minimum number of generators of a group  $G$ .

**Corollary 2.5.** *The following hold for  $g \in \mathbb{Z}_{\geq 1}$  and  $p, n \in \mathbb{Z}_{\geq 2}$ .*

- (1)  $\text{hc}(X) = 0$  if and only if  $H_1(X) = 0$ .
- (2)  $\text{hc}(X) = g$  if  $H_1(X)$  is isomorphic to  $\mathbb{Z}^{2g-1}$  or  $\mathbb{Z}^{2g}$ .
- (3)  $\text{hc}(X) = 1$  if  $H_1(X) \cong \mathbb{Z}/p$ .
- (4) If  $X$  is a rational homology 3-sphere and the subgroup of  $H_1(X)$  consisting of 2-torsions is cyclic (possibly trivial), then  $\text{hc}(X) \leq d(H_1(X))$ .
- (5)  $\text{hc}(L(p_1, q_1) \sharp L(p_2, q_2)) = 2$  if  $p_1$  divides  $p_2$  and  $|q_1 q_2|$  is not a quadratic residue mod  $p_1$ .
- (6) Suppose  $H_1(X) \cong \mathbb{Z} \oplus \mathbb{Z}/p$ . Then,  $\text{hc}(X) = 1$  if there is  $q \in \mathbb{Z}$  such that the torsion linking form  $\lambda_X$  is isomorphic to  $(q/p)$  and  $q$  or  $-q$  is a quadratic residue mod  $p$ . Otherwise,  $\text{hc}(X) = 2$ .

**Remark 2.6.** Combining (4) and well-known inequalities, under the assumption of (4), we have

$$\text{hc}(X) \leq d(H_1(X)) \leq d(\pi_1(X)) \leq g(X) \leq 2 \text{op}(X),$$

where  $g(X)$  denotes the Heegaard genus of  $X$ . On the other hand,  $\text{hc}(X) \leq \text{op}(X)$  and  $\text{hc}(X \sharp Y) \leq \text{hc}(X) + \text{hc}(Y)$  hold for any  $X, Y$  by definition, and  $d(H_1(X)) \leq 2 \text{hc}(X)$  is found in [8, Remark 6.1].

*Proof of Corollary 2.5.* (1) is obvious, (2) is due to Sakasai [8], and (3) is a direct consequence of Theorem 1.1 since  $\lambda_X$  is isomorphic to  $\lambda_{L(p, q)}$  for some  $q$ .

We next prove (4). Since  $H_1(X)$  is finite, it is isomorphic to  $\bigoplus_{i=1}^s \mathbb{Z}/p_i$  for some  $p_i$ 's with  $p_i \mid p_{i+1}$ , where  $s := d(H_1(X))$ . It follows from [10, Theorem (4)] that  $\lambda_X$  is isomorphic to  $\bigoplus_{i=1}^s (q_i/p_i)$  for some  $q_i$ 's, hence  $\lambda_X$  is isomorphic to  $\lambda_{L(p_1, q_1) \sharp \dots \sharp L(p_s, q_s)}$ . Therefore, Theorem 1.1 shows  $\text{hc}(X) \leq s$ . The proofs of (5) and (6) are given in Section 4.  $\square$

## 3. PROOF OF THEOREM 1.2

The goal of this section is to prove Theorem 1.2 which is used in the proof of Theorem 1.1. We briefly review the Artin symbol of a prime ideal only for the case of abelian extensions following [5, Chapter X, Section 1] and [7, Chapter VI, Section 7]. Let  $k$  be an algebraic number field,  $K/k$  be an abelian extension, namely it is a finite Galois extension whose Galois group  $G = \text{Gal}(K/k)$  is abelian. Let  $\mathfrak{p} \neq 0$  be an unramified prime ideal of  $\mathfrak{o}_k$ , the ring of integers of  $k$ , let  $\mathfrak{P}$  be a prime ideal of  $\mathfrak{o}_K$  lying above  $\mathfrak{p}$ , that is,  $\mathfrak{P} \cap k = \mathfrak{p}$ . Then there exists a unique element of the decomposition group  $\{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$  of  $\mathfrak{P}$  satisfying  $\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$  for all  $x \in \mathfrak{o}_K$ , where  $N(\mathfrak{p}) := [\mathfrak{o}_k : \mathfrak{p}] \in \mathbb{Z}_{\geq 1}$ . This automorphism is independent of the choice of  $\mathfrak{P}$ , which is denoted by  $\left(\frac{K/k}{\mathfrak{p}}\right)$  and called the *Artin symbol* of  $\mathfrak{p}$ .

**Example 3.1** ([5, Chapter X, Section 1]). We review two well-known examples used in this paper. Let  $a \in \mathbb{Z}$  be not a perfect square,  $\Delta_a$  be the discriminant of  $\mathbb{Q}(\sqrt{a})$ ,  $p$  be a prime with  $\gcd(\Delta_a, p) = 1$ . Then,  $p\mathbb{Z}$  is unramified and we deduce

$$\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p\mathbb{Z}}\right) = \begin{cases} \text{id}_{\mathbb{Q}(\sqrt{a})} & \text{if } \Delta \text{ is a quadratic residue mod } p, \\ [\sqrt{a} \mapsto -\sqrt{a}] & \text{otherwise.} \end{cases}$$

Next, for a primitive  $n$ th root of unity  $\zeta_n$  and a prime  $p$  with  $\gcd(n, p) = 1$ , the ideal  $p\mathbb{Z}$  is unramified and  $\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p\mathbb{Z}}\right) = [\zeta_n \mapsto \zeta_n^p]$  holds.

**Lemma 3.2.** *Let  $K_1/k, K_2/k$  be abelian extensions,  $C$  be a subset of  $G_1 \times G_2$  with  $\iota^{-1}(C) \neq \emptyset$ , where  $G_i$  denotes  $\text{Gal}(K_i/k)$  and  $\iota: \text{Gal}(K_1K_2/k) \rightarrow G_1 \times G_2$  is defined by  $\iota(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$ . Then the set*

$$S := \left\{ \mathfrak{p} \mid \begin{array}{l} \mathfrak{p} \text{ is an unramified} \\ \text{prime ideal of } \mathfrak{o}_k \end{array} \text{ and } \left( \left( \frac{K_1/k}{\mathfrak{p}} \right), \left( \frac{K_2/k}{\mathfrak{p}} \right) \right) \in C \right\}$$

*is infinite.*

*Proof.* First note that  $K_1K_2/k$  is a Galois extension with  $G = \text{Gal}(K_1K_2/k)$  abelian, and the homomorphism  $\iota: G \rightarrow G_1 \times G_2$  is injective. We define the set  $S'$  by

$$S' := \left\{ \mathfrak{p} \mid \begin{array}{l} \mathfrak{p} \text{ is an unramified} \\ \text{prime ideal of } \mathfrak{o}_k \end{array} \text{ and } \left( \frac{K_1K_2/k}{\mathfrak{p}} \right) \in \iota^{-1}(C) \right\}.$$

By the Chebotarev density theorem (see, for example, [5, Chapter VIII, Theorem 10], [7, Chapter VII, Theorem 13.4]), we have  $d(S') = |\iota^{-1}(C)|/|G| > 0$ , where  $d(S')$  is the Dirichlet density of  $S'$  (see [5, Chapter VIII, Section 4], [7, Chapter VII, Section 13]). Hence,  $S'$  is infinite. On the other hand, the consistency property [5, Chapter X, Section 1] asserts  $S' \subset S$ , and thus  $S$  is also infinite.  $\square$

**Lemma 3.3.** *For  $a, m, n \in \mathbb{Z}$  with  $\sqrt{a} \notin \mathbb{Q}(\zeta_n)$  and  $\gcd(m, n) = 1$ , the set  $S := \{p \mid p \text{ is a prime, } a \text{ is a quadratic residue mod } p \text{ and } p \equiv m \pmod{n}\}$*

is infinite.

*Proof.* Put  $k = \mathbb{Q}$ ,  $K_1 = k(\sqrt{a})$ ,  $K_2 = k(\zeta_n)$  and  $C = \{(\text{id}_{K_1}, [\zeta_n \mapsto \zeta_n^m])\}$ . Since  $K_1 \cap K_2 = k$ , the map  $\iota$  in Lemma 3.2 is an isomorphism, and thus  $\iota^{-1}(C) \neq \emptyset$ . It follows from Lemma 3.2 that

$$\left\{ p \left| \begin{array}{l} p > \max\{\Delta_a, n\} \\ \text{is a prime} \end{array} \right. , \left( \frac{K_1/k}{p\mathbb{Z}} \right) = \text{id}_{K_1} \text{ and } \left( \frac{K_2/k}{p\mathbb{Z}} \right) = [\zeta_n \mapsto \zeta_n^m] \right\}$$

is infinite. Here, Example 3.1 implies that this set is included in  $S$ .  $\square$

**Lemma 3.4.** *For a positive integer  $n \neq 5$ ,  $\sqrt{n(n+4)}$  or  $\sqrt{n(n-4)}$  does not belong to the  $n$ th cyclotomic field  $\mathbb{Q}(\zeta_n)$ .*

*Proof.* The cases  $n = 1, 2$  are obvious. For  $n > 2$ , we consider four cases: (I)  $v_2(n) = 0$ , (II)  $v_2(n) = 1$ , (III)  $v_2(n) = 2$ , (IV)  $v_2(n) \geq 3$ , where  $v_2$  is the 2-adic valuation for  $\mathbb{Z}$ . We only discuss (I), and the other cases are shown similarly. In general,  $\sqrt{a} \in \mathbb{Q}(\zeta_n)$  if and only if  $a \in \mathbb{Z}$  is a product of some integers in

$$\{(-1)^{(p-1)/2}p \mid p \text{ is an odd prime factor of } n\}.$$

(See, for example, [11, Corollary 4.5.4]). Since  $\gcd(n, n \pm 4) = 1$ , both  $n+4$  and  $n-4$  must be perfect squares, though that is impossible except  $n = 5$ .  $\square$

*Proof of Theorem 1.2.* It follows from Lemmas 3.3 and 3.4 that there are  $\varepsilon \in \{1, -1\}$  and an odd prime  $l$  such that  $n(n+4\varepsilon)$  is a quadratic residue mod  $l$  and  $l \equiv m \pmod{n}$ . Therefore, by  $\gcd(l, n) = 1$ ,  $n(n+4\varepsilon)$  is a quadratic residue mod  $l$  if and only if  $(2nx+n)^2 \equiv n^2 + 4\varepsilon n \pmod{l}$  is solvable. Moreover, this congruence equation is equivalent to  $nx(x+1) \equiv \varepsilon \pmod{l}$ .  $\square$

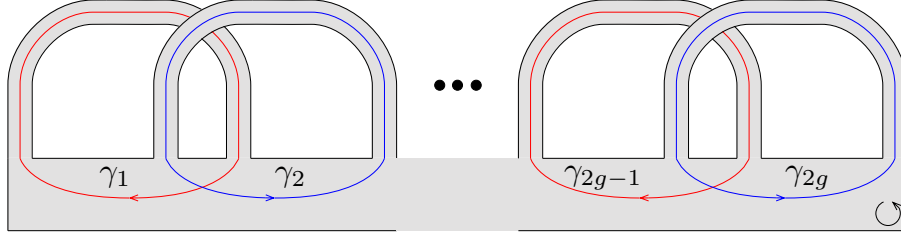
**Remark 3.5.** The above proof (and the case  $p = 5$  in the proof of Theorem 1.1) claims that for any  $L(p, q')$  there exists  $q \in \mathbb{Z}$  such that  $L(p, q)$  is homeomorphic to  $L(p, q')$  and Sakasai's sufficient condition in Section 1 is true for  $q$ .

Even if  $n = 5$ , Theorem 1.2 holds for  $m \equiv 1, 3, 4 \pmod{5}$ . Indeed, one can choose  $(\varepsilon, l) = (-1, 11), (1, 3), (1, 19)$  respectively. However, in the case  $m \equiv 2 \pmod{5}$ , Theorem 1.2 fails since neither  $5(5+4)$  nor  $5(5-4)$  is a quadratic residue mod  $m$  by the quadratic reciprocity law.

#### 4. HOMOLOGICALLY FIBERED KNOTS AND THE ALEXANDER POLYNOMIAL

We discuss homologically fibered knots which are defined in terms of homology cobordisms. Seifert matrices of connected oriented surfaces in a rational homology 3-sphere  $Y$  play a key role in this section.

Let  $\iota: \Sigma_{g,1} \xrightarrow{\cong} \Sigma \subset Y$  be an embedding and  $S = (s_{ij})_{i,j} \in M_{2g}(\mathbb{Q})$  be the Seifert matrix of  $\Sigma$  with respect to  $\{\iota(\gamma_1), \dots, \iota(\gamma_{2g})\}$  (see Figure 4.1), that is,  $s_{ij} = \text{lk}_Y(\iota(\gamma_i), \gamma_j^+)$ , where  $\gamma_j^\pm := \iota^\pm(\gamma_j)$ . Note that, in the next proposition,

FIGURE 4.1. Oriented curves  $\gamma_1, \dots, \gamma_{2g}$  on the surface  $\Sigma_{g,1}$ .

$S$  cannot be regarded as the matrix of  $(\iota^+)_*$  unlike in [4, Proposition 3.2] since  $S \notin M_{2g}(\mathbb{Z})$  in general.

**Proposition 4.1.**  *$(Y \setminus \text{Int}(\Sigma \times [-1, 1]), \iota^-, \iota^+)$  is a homology cobordism if and only if  $|\det S| = |H_1(Y)|^{-1}$  and  $\text{Im}(\iota^+)_* \subset \text{Im}(\iota^-)_*$ .*

*Proof.* Suppose that  $Y \setminus \text{Int} \tilde{\Sigma}$  is a homology cobordism, where  $\tilde{\Sigma} := \Sigma \times [-1, 1]$ . Then one can consider the matrix  $M \in GL(2g, \mathbb{Z})$  of the automorphism  $f := (\iota^-)^{-1}_* \circ (\iota^+)_*$  with respect to  $\{[\gamma_1], \dots, [\gamma_{2g}]\}$  and check that  $S^T M = S$  similar to the case  $Y = S^3$ . We have

$$\det(S^T) \det(M - I_{2g}) = \det(S - S^T) = \det \bigoplus_{i=1}^g \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = 1,$$

hence  $|\det S| = |H_1(Y)|^{-1}$  is equivalent to  $|\text{Coker}(M - I_{2g})| = |H_1(Y)|$ , and it suffices to show that

$$(B :=) \{f(x) - x \mid x \in H_1(\Sigma_{g,1})\} = \text{Im}[\partial_* : H_2(Y, \Sigma) \rightarrow H_1(\Sigma_{g,1})].$$

The inclusion  $\subset$  follows from  $\iota_*(f(x) - x) = 0$ . Next, for any  $y \in H_2(Y, \Sigma) \cong H_2(Y \setminus \text{Int} \tilde{\Sigma}, \partial \tilde{\Sigma})$  let  $S_y$  be an immersed surface satisfying  $[S_y] = y$  and  $S_y \cap \Sigma \subset \partial S_y$ . Then  $\partial S_y$  consists of two types of closed curves: curves coming from  $\Sigma \times \{1\}$  and ones coming from  $\Sigma \times \{-1\}$ . Let  $x_\sigma \in H_1(\Sigma)$  be the class of the curves coming from  $\Sigma \times \{\sigma\}$ . We have

$$(\iota^-)_*(f(x_+) + x_-) = (\iota^+)_*(x_+) + (\iota^-)_*(x_-) = [\partial S_y] = 0 \in H_1(Y \setminus \text{Int} \tilde{\Sigma}).$$

Therefore,  $\partial_*(y) = x_+ + x_- = f(-x_+) - (-x_+) \in B$ .

We next prove the converse. First note that  $\det S \neq 0$  claims that  $(\iota^\pm)_*$  are injective, and thus there is a unique endomorphism  $f$  of  $H_1(\Sigma_{g,1})$  satisfying  $(\iota^-)_* \circ f = (\iota^+)_*$ . This equality implies  $\iota_*(B) = 0$ , hence we have the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & B & \longrightarrow & H_1(\Sigma_{g,1}) & \longrightarrow & H_1(\Sigma_{g,1})/B \longrightarrow 0 \text{ (exact)} \\ & & \downarrow (\iota^\pm)_* & \nearrow & \downarrow (\iota^\pm)_* & & \downarrow \iota^-_* \\ 0 & \longrightarrow & \text{Im } \partial_* & \xrightarrow{\text{incl}} & H_1(Y \setminus \text{Int} \tilde{\Sigma}) & \longrightarrow & H_1(Y) \longrightarrow 0 \text{ (exact)}. \end{array}$$

Here, if one shows that the map  $\text{incl}$  lifts to a map

$$\text{Im}[\partial_* : H_2(Y, Y \setminus \text{Int} \tilde{\Sigma}) \rightarrow H_1(Y \setminus \text{Int} \tilde{\Sigma})] \dashrightarrow H_1(\Sigma_{g,1}),$$



then  $(\iota^\pm)_*$  are isomorphisms, hence  $\overline{\iota}_*$  is injective. Finally, the assumption  $|\det S| = |H_1(Y)|^{-1}$  says that  $\overline{\iota}_*$  is an isomorphism, and so are  $(\iota^\pm)_*$  by the five lemma.

For any  $y \in \text{Im } \partial_*$ , the excision isomorphism  $H_2(Y, Y \setminus \text{Int } \tilde{\Sigma}) \cong H_2(\tilde{\Sigma}, \partial \tilde{\Sigma})$  asserts that there is an immersed surface  $S_y$  in  $\tilde{\Sigma}$  satisfying  $\partial S_y \subset \Sigma \times \{1, -1\}$  and  $[\partial S_y] = y$ . Let  $x_+ \in H_1(Y \setminus \text{Int } \tilde{\Sigma})$  (resp.  $x_-$ ) be the class of the curves  $\partial S_y \cap \Sigma \times \{1\}$  (resp.  $\partial S_y \cap \Sigma \times \{-1\}$ ). We see that  $x_\pm \in \text{Im}(\iota^\pm)_*$ , and therefore  $(\iota^-)_*(f((\iota^+)^{-1}_*(x_+)) + (\iota^-)^{-1}_*(x_-)) = x_+ + x_- = y$ .  $\square$

*Alternative proof of Lemma 2.3.* It is easy to see that the Seifert matrix  $S$  of  $\Sigma = \Sigma_{a,b,c,u,v}$  with respect to  $\{\alpha, \beta\}$  is

$$\begin{pmatrix} a + \frac{q}{p}u^2 & c - \frac{q}{p}uv \\ c + 1 - \frac{q}{p}uv & b + \frac{q}{p}v^2 \end{pmatrix},$$

and we have

$$\det S = -(c^2 + c - ab) + \frac{q}{p}(bu^2 + (2c + 1)uv + av^2).$$

Therefore, if the complement is a homology cobordism, then Proposition 4.1 shows that there are  $\varepsilon$  and  $k$  in Lemma 2.3. Conversely, the existence of  $\varepsilon$  and  $k$  implies that  $|\det S| = 1/p$  and  $\alpha', \beta' \in \text{Im}(\iota^-)_*$ , hence we have  $\text{Im}(\iota^+)_* \subset \text{Im}(\iota^-)_*$ .  $\square$

The following terminology was introduced by Goda and Sakasai [4, Definition 3.1] in the case  $X = S^3$  (see also [8, Definition 7.1]).

**Definition 4.2.** An oriented knot  $K$  in a connected oriented closed 3-manifold  $X$  is called a *homologically fibered knot of genus  $g$*  if there is a Seifert surface of  $K$  such that  $X \setminus \text{Int}(\Sigma \times [-1, 1])$  is a homology cobordism over  $\Sigma_{g,1}$ .

By definition,  $\text{hc}(X) = g$  if and only if  $X$  contains a homologically fibered knot of genus  $g$ , but does not contain one of genus  $g - 1$ .

**Remark 4.3.** If  $X$  is a rational homology 3-sphere, then Corollary 4.5 shows that  $g$  in Definition 4.2 must be equal to the knot genus  $g(K)$  of  $K$ .

We next see that the Alexander polynomial  $\Delta_K(t)$  of an oriented null-homologous knot  $K$  in a rational homology 3-sphere  $Y$  gives a necessary condition for  $K$  to be homologically fibered. Recall that  $\Delta_K(t)$  is defined by

$$\Delta_K(t) := \det(t^{1/2}S - t^{-1/2}S^T) \in \mathbb{Q}[t, t^{-1}],$$

where  $S$  is a Seifert matrix of a Seifert surface  $\Sigma$  of  $K$ . By definition,  $\Delta_K(t)$  should be palindromic and satisfy  $\Delta_K(1) = 1$ , and its breadth is less than or equal to  $2g(K)$ .

**Example 4.4.** Suppose that  $L(p, q) \setminus \text{Int}(\Sigma_{a,b,c,u,v} \times [-1, 1])$  is a homology cobordism (see Figure 2.1). Then there exists  $\varepsilon \in \{1, -1\}$  in Lemma 2.3, for the knot  $K = \partial\Sigma_{a,b,c,u,v}$  in  $L(p, q)$ , we have

$$\Delta_K(t) = 1 - \frac{\varepsilon}{p}(t - 2 + t^{-1}).$$

**Corollary 4.5.** *If an oriented knot  $K$  in  $Y$  is homologically fibered, then the breadth of  $\Delta_K(t)$  equals  $2g(K)$  and the coefficient of the highest degree term equals  $|H_1(Y)|^{-1}$  up to sign.*

*Proof.* In general, for  $S \in GL(2g, \mathbb{Q})$  the highest degree term of  $\det(t^{1/2}S - t^{-1/2}S^T)$  is equal to  $(\det S)t^g$ . Therefore, Proposition 4.1 proves the corollary.  $\square$

Finally, we complete the rest of the proof of Corollary 2.5 by using Theorem 1.1, Proposition 4.1 and the following remark.

**Remark 4.6.** Let  $\Sigma'$  be a surface in  $X$  obtained from  $\Sigma = \iota(\Sigma_{g,1})$  by two crossing changes between  $\iota(\gamma_i)$  and  $\iota(\gamma_j)$  with opposite sign. Then a Mayer-Vietoris argument shows that if the complement of  $\Sigma$  is a homology cobordism, then so is the complement of  $\Sigma'$ .

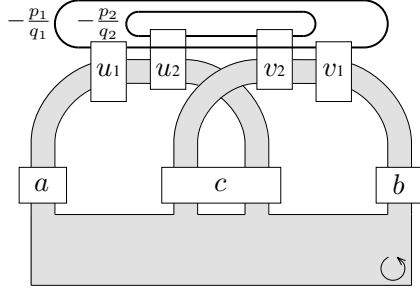


FIGURE 4.2. The surface  $\Sigma_{a,b,c,u_1,u_2,v_1,v_2} \subset L(p_1, q_1) \# L(p_2, q_2)$ , where the indices of  $\Sigma$  are integers like Figure 2.1.

*Proofs of Corollary 2.5 (5), (6).* (5) For  $X = L(p_1, q_1) \# L(p_2, q_2)$  with  $p_1 \mid p_2$ , by Theorem 1.1, we know that  $\text{hc}(X)$  equals 1 or 2. Remark 4.6 allows us to find a surface of the form  $\Sigma_{a,b,c,u_1,u_2,v_1,v_2}$  (see Figure 4.2) whose complement is a homology cobordism. The Seifert matrix  $S$  of  $\Sigma_{a,b,c,u_1,u_2,v_1,v_2}$  is given by

$$S = \begin{pmatrix} a + \frac{q_1}{p_1}u_1^2 + \frac{q_2}{p_2}u_2^2 & c - \frac{q_1}{p_1}u_1v_1 - \frac{q_2}{p_2}u_2v_2 \\ c + 1 - \frac{q_1}{p_1}u_1v_1 - \frac{q_2}{p_2}u_2v_2 & b + \frac{q_1}{p_1}v_1^2 + \frac{q_2}{p_2}v_2^2 \end{pmatrix} \in \frac{1}{p_2}M_2(\mathbb{Z}),$$

and it follows from Proposition 4.1 that

$$1 = |H_1(X)| |\det S| \equiv |q_1 q_2| (u_1 u_2 - v_1 v_2)^2 \pmod{p_1}.$$

Thus,  $|q_1 q_2|$  is a quadratic residue mod  $p_1$ .

(6) We may assume that  $X = (S^1 \times S^2) \sharp L(p, q)$ . By Theorem 1.1, it suffices to prove that  $\text{hc}(X) = 1$  if and only if  $q$  or  $-q$  is a quadratic residue mod  $p$ . Suppose  $\text{hc}(X) = 1$ . There is  $A \in SL(2, \mathbb{Z})$  such that the closure  $C$  of the homology cobordism  $(\Sigma_{1,1} \times [-1, 1], \text{incl}, \tilde{A})$  is Borromean surgery equivalent to  $X$ , where  $\tilde{A}$  is a homeomorphism of  $\Sigma_{1,1}$  inducing  $A$  on  $H_1(\Sigma_{1,1})$  (see [8, Section 6.3]). Here we have  $\det(A - I_2) = 0$  since the Mayer-Vietoris sequence for  $C = \Sigma_{1,1} \times [-1, 0] \cup \Sigma_{1,1} \times [0, 1]$  shows  $\text{Coker}(A - I_2) \cong H_1(C)$ . Therefore, by the proof of [9, Proposition 2],  $A$  is conjugate to  $\begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$  in  $SL(2, \mathbb{Z})$  for some  $u \in \mathbb{Z}$ . Now,  $u$  must be  $\varepsilon p$  for some  $\varepsilon \in \{1, -1\}$ , then  $\tilde{A}$  can be chosen so that  $C \cong (S^1 \times S^2) \sharp L(p, -\varepsilon)$ . Thus the torsion linking form  $(q/p)$  is isomorphic to  $(-\varepsilon/p)$ .

In particular, the above argument implies that  $(S^1 \times S^2) \sharp L(p, \varepsilon)$  is the closure of a homology cobordism over  $\Sigma_{1,1}$ , which proves the converse.  $\square$

## REFERENCES

- [1] A. Baker. *A comprehensive course in number theory*. Cambridge University Press, Cambridge, 2012.
- [2] K. L. Baker. Counting genus one fibered knots in lens spaces. *Michigan Math. J.*, 63(3):553–569, 2014.
- [3] S. Garoufalidis and J. Levine. Tree-level invariants of three-manifolds, Massey products and the Johnson homomorphism. In *Graphs and patterns in mathematics and theoretical physics*, volume 73 of *Proc. Sympos. Pure Math.*, pages 173–203. Amer. Math. Soc., Providence, RI, 2005.
- [4] H. Goda and T. Sakasai. Homology cylinders and sutured manifolds for homologically fibered knots. *Tokyo J. Math.*, 36(1):85–111, 2013.
- [5] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.
- [6] K. Morimoto. Genus one fibered knots in lens spaces. *J. Math. Soc. Japan*, 41(1):81–96, 1989.
- [7] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
- [8] T. Sakasai. Johnson-Morita theory in mapping class groups and monoids of homology cobordisms of surfaces, available at <http://www.ms.u-tokyo.ac.jp/~sakasai/index.html>.
- [9] M.-o. Takahashi and M. Ochiai. Heegaard diagrams of torus bundles over  $S^1$ . *Comment. Math. Univ. St. Paul.*, 31(1):63–69, 1982.
- [10] C. T. C. Wall. Quadratic forms on finite groups, and related topics. *Topology*, 2:281–298, 1963.
- [11] S. H. Weintraub. *Galois theory*. Universitext. Springer, New York, second edition, 2009.

GRADUATE SCHOOL OF MATHEMATICAL SCIENCES, THE UNIVERSITY OF TOKYO, 3-8-1  
KOMABA, MEGURO-KU, TOKYO, 153-8914, JAPAN  
E-mail address: nozaki@ms.u-tokyo.ac.jp